Appendix A: Technology Specific Information

This section contains technology-specific information for each packet-mode technology discussed in the JEM. The JEM did not receive contributions for all possible packet technologies; therefore, not all packet technologies are represented in this section. The section is broken into two parts:

- Access Networks: this section and its subsections contain descriptions of information that can be delivered for various types of networks used to access packet-mode networks. This includes the following technologies:

  - cdma2000
  - GPRS
  - CDPD
  - Packet Cable

It was recognized that dial-up access to the Internet was the main method for accessing the Internet for most users, but there were no contributions for this method.

- Network Protocols: this section contains descriptions of information that can be delivered for various packet-mode protocols. The following protocols were covered:

  - X.25
  - IP
  - ATM
  - Frame Relay

A.1 Access networks

A.1.1 Call Associated Signaling Reporting

A.1.1.1 Reporting Call Associated Information

Future wireless systems may be supporting Voice over IP (VoIP) calls via new signaling methods such as SIP and H.323. In these scenarios, a call client in the handset communicates with a call server controlled by the accessing system to establish a voice call using packet-mode communication. The accessing system may then interwork the VoIP call into the PSTN using signaling and media gateways (e.g., RTP-TDM, SIP-SS7) or deliver the call directly into a network using packet-mode communication (e.g., SIP, RTP). Call associated information can be reported in these scenarios. Two methods have been identified:

a) Reporting J-STD-025 Call Associated Events

With this method, call associated signaling such as SIP/H.323 would be mapped to the J-STD-025 call events.[2] The development of this method is required in order to provide backward compatibility for systems that incorporate the J-STD-025 capabilities. This method will require changes and enhancements to J-STD-025.[3]

b) Reporting SIP/H.323 Signaling

With this method, the actual call associated signaling is reported to the LEAs. This alternate capability may be advantageous to future systems that do not have a backward compatibility issue with the J-STD-025 call events. The following information could be reported:

- Call Session ID (e.g., Call ID);
- Call Session Information Type (e.g., H.323 family signaling, SIP signaling); and
- Call Session Information.

[2] See J-STD-025 Section 4.4 Call Associated Information Surveillance Service Description - Call Identifying Information IAP (IDIAP) and the listed call events.

[3] Currently in J-STD-025 the IDIAP call events are defined only for circuit-mode calls. In addition, these events may not be able to carry all necessary packet-mode VoIP information (e.g., Session Definition Protocol information).

A.1.2 cdma2000

A.1.2.1 Overview

The cdma2000 Wireless IP service offering is described in TIA/EIA/IS-835. This standard specifies a system that will provide IPv4 service over a cdma2000 radio network. Two types of service are described, namely Simple IP, which provides IP service within a network much like traditional dial-up IP service, and Mobile IP, which provides persistent IP service across all connected networks. The Wireless IP system only provides for transport of IPv4 packets, and does not offer any higher level functions for communication services within the standardized system. High level figures depicting the various network elements for these two services are shown in Figures 1.

Network elements that are specific to the cdma2000 Wireless IP Network are the Packet Data Serving Node (PDSN), the RADIUS servers [RFC2138], and the Home Agent (HA). The PDSN and local RADIUS server are part of the serving wireless network, while the home and broker RADIUS servers and HA may be part of another IP network (e.g., another wireless network, or private network). The RADIUS servers provide the authentication, authorization and accounting functions and use a Network Access Identifier (NAI) of the form user@realm to identify subscribers. Separate authentication, authorization and accounting are provided via the Radio Network using standard wireless Visitor Location Register (VLR) and Home Location Register (HLR). This information, however, is not communicated with the Wireless IP network elements.

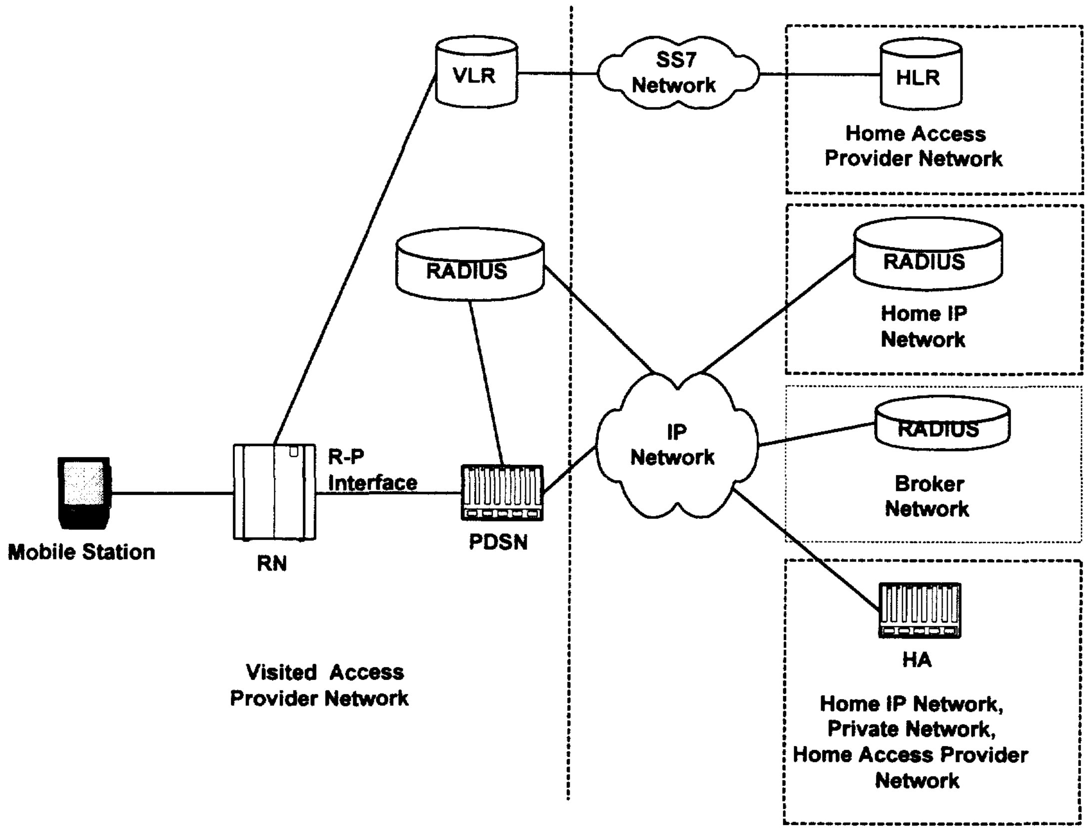

Figure 1: Reference Model (HA only for with Mobile IP service)

A.1.2.2 Technical Capabilities for support of CALEA

Since the cdma2000 Wireless IP system only provides basic transport of IPv4 packets and does not provide communication services such as Voice over IP which require a call management server, it is limited in its ability to report specific Pen Register and Trap and Trace information. The network is unaware of any underlying services that are running between the user and any correspondent nodes, and as such is unable to report call events. As such, the cdma2000 Wireless IP system capabilities are consistent with those referenced within the JEM report under the section Packet Communication Sessions established without a Call Management Server.

A.1.2.3 Reporting of Call Information

The cdma2000 packet data architecture as described in IS-835 "Wireless Packet Data Standard" provides informational services and as such may act as a bearer service for communication services. The standard does not describe the applications that are supported in the network, nor does it describe how to interpret the packet data information based on the application since this varies widely between different applications. This information is unnecessary and beyond the scope of the standards since the intent is to provide packet data "access." It is not technically feasible to determine, either on a packet by packet basis or on a stream basis, the application or communication service being used. Furthermore, the possibility of encapsulation or encryption of packets outside of the network makes identifying the application or service even more unlikely. Therefore, the level of complexity required of the network to attempt to extract Pen Register or Trap and Trace information from information services is not feasible.

The system is capable of providing copies of the full IP packets to law enforcement for a limited number of subjects, given the constraints detailed below in the System Performance Impacts section. The system could also provide only the outermost IP routing headers (e.g. commonly referred to as IP headers), which, as discussed in the JEM report, may not provide any significant value. In either case, however, the system is unable to differentiate those packets which are associated with a telecommunications service from those that are associated with an information service and as such must deliver all or none of the packets associated with a given user. It should be noted that in some loading situations a user might be able to detect performance degradation resulting from this service, and that a single heavy user may occupy a disproportionate amount of system resources.

A.1.2.4 Reporting of Access Control Information

Similar to wireline systems, wireless systems establish a communication path across the accessing system from the subject's device to a network before communication between subject and associate can begin. The establishment and release of this path corresponds to establishment and termination of packet data service and could be reported when an intercept subject has established communication ability.

The following events could be reported:

- packet data service establishment;
- packet data service termination;
- start of interception with packet data service active ; and
- PCF handoff.

A.1.2.5 Target and Associate Identity

End users can be identified by either the NAI or their MSID. Since the MSID is not used in the Wireless IP system, the NAI is the most appropriate form of identification. Because the IP address of a target may be dynamically assigned on a per session basis, it is not practical to just identify the subject by an IP address. The system can determine on a real time basis the IP address that has been assigned to the NAI associated with a subject for that session and then perform further interception based on that IP address. It should be noted that the architecture specified in TIA/EIA/IS-835 allows for multiple users (in the case of externally connected devices) to access the packet data network through a single terminal. It should be further noted that the home network for the NAI may or may not belong to a wireless service provider, that a user may have multiple NAIs which can be used to access the network, and that the NAI is not tied to use on a single terminal.

After a communication path is established by a wireless accessing system between the subject device(s) and network, the subject can communicate directly with many associates over the connecting path. The associates with whom the subject is communicating can only be identified within the Wireless IP network by the corresponding IP addresses – no further information is available to the network. These addresses may be of a transitive nature since the associates could have a dynamically assigned address, and the true associates may only be identified by additional information in the payload of the packet and not the corresponding IP address.

A.1.2.6 Point of Interception

There are several points in the network where the user information transiting the system may be intercepted. These include components within the visited access network where the target is being provided packet data transport service, and components within the home network which provide additional services. Due to the nature of communication flows for Simple IP and Mobile IP services, the recommended point of interception is in the visited access network at the Packet Data Serving Node (PDSN). By intercepting at the visited PDSN, all information flowing between a subject and associate for both Simple IP and Mobile IP may be monitored and all relevant user identifying information is readily available. Some serving system information may be obtained from the home network HLR and Home AAA servers as described later in this section. Note however, that the home AAA server may reside in a network other than one belonging to a telecommunications service provider.

A.1.2.7 Serving System Message

In the LAES for CALEA standard, J-STD-025, a non-call associated surveillance service was defined to access information within a telecommunication system. The non-call associated information identified was Serving System information for personal or terminal mobility. The Serving System message in this standard provides information as to the roaming system assigned to provide service for the mobile subscriber.

The mobile gains access to the cdma2000 network via the CDMA network and the subscription to the packet data service. The home network (HLR) could advise law enforcement of the network where the subscriber is now roaming, but may not have knowledge that the subject is using the packet data service subscription. However, the home AAA could advise law enforcement, in a similar fashion, that the subject is being provided packet data service by a foreign network and the IP address of PDSN providing access. In summary, serving system information for MSID based lawful interception may be obtained at the HLR while serving system information for NAI based lawful interception may be obtained from the Home AAA server.

A.1.2.8 Method of Delivery to Law Enforcement

Given that the PDSN and home AAA servers are network elements in an IP based network, the most logical and preferred method for communicating information to law enforcement is via an IP network connection. Access Control and Serving system information could be standardized for transmission within an IP packet, and if copies of the full packets are provided, the contents of the communication stream could be encapsulated in a standard IP tunnel.

A.1.3 General Packet Radio Service

A.1.3.1 Overview

General Packet Radio Service (GPRS) is a packet-mode access technique for mobile subscribers providing the transfer of high and low speed data and signaling. Interworking is defined with IP and X.25 networks. Point-to-Point (PTP) and Point-to-Multi-point (MTP) applications are supported along with multiple quality of service profiles for the subscriber. The GPRS allows the service subscriber to send and receive data in an end-to-end packet transfer mode, without utilizing network resources in circuit switched mode.

The following are a number of possible PTP interactive teleservices:

- retrieval services, which provide the capability of accessing information stored in data, base centers. The information is sent to the user on demand only. An example of one such service in the Internet's World Wide Web (WWW);

- messaging services, which offer user-to-user communication between individual users via storage units with store-and-forward mailbox, and/or message handling (e.g., information editing, processing and conversion) functions;

- conversational services which provide bi-directional communication by means of real-time (no store-and-forward) end-to-end information transfer from user to user. An example of such a service is the Internet's Telnet application;

- tele-action services which are characterized by low data-volume (short) transactions, for example credit card validations, lottery transactions, utility meter readings and electronic monitoring and surveillance systems.

Some examples of teleservices that may be supported by a PTM bearer service include:

- distribution services, which are characterized by the unidirectional, flow of information from a given point in the network to other (multiple) locations. Examples may include news, weather and traffic reports, as well as product or service advertisements;

- dispatching services which are characterized by the bi-directional flow of information from a given point in the network (dispatcher) and other (multiple) users. Examples include taxi and public utility fleet services;

- conferencing services which provide multi-directional communication by means of real-time (no store-and-forward) information transfer between multiple users.

Capabilities that may be offered together with the PTM bearer services include:

- geographical routing capability, which provides the ability to restrict message distribution to a specified geographical area;

- scheduled delivery capability, allowing store-and-forward type services to specify a future delivery time and a repetition rate.

It is possible to include these capabilities as part of the service request (i.e., as part of the packet). Some operators may offer PTM services only together with these capabilities.

GPRS defines two new interconnected network nodes:

a) A Serving GPRS Support Node (SGSN) which keeps track of the individual Mobile Station's (MS's) location and performs security functions and access control. The SGSN performs authentication and cipher setting procedures.

b) A Gateway GPRS Support Node (GGSN) which provides interworking with external packet-switched networks.

The GSM Home Location Register (HLR) is enhanced with GPRS subscriber information and the Short Message Service (SMS) Gateway MSC (GMSC) and SMS Interworking MSC (SMS-IWMSC) are upgraded to support SMS transmission via the SGSN. GPRS security functionality is equivalent to the existing GSM security.

The MS informs the network when it re-selects another cell or group of cells known as a routing area.

In order to access the GPRS services, an MS must first make its presence known to the network by performing a GPRS attach. This operation establishes a logical link between the MS and the SGSN and makes the MS available for SMS over GPRS, paging via SGSN, and notification of incoming GPRS data.

In order to send and receive GPRS data, the MS must activate the packet data address that it wants to use. This operation makes the MS known in the corresponding GGSN and interworking with external data networks can commence.

User data is transferred transparently between the MS and the external data via encapsulation and tunneling techniques. This transparent transfer method lessens the requirement to interpret external data protocols and enables easy introduction of additional interworking protocols in the future.

For GPRS the following information could be provided to the LEAs separately from the call content:

- an activation reference identity;
- the target identity which has been intercepted (e.g., MSISDN, IMSI, IMEI if applicable);

- type of protocol activated (e.g., Internet Protocol or X.25);
- PDP address used by the target (e.g., IP Address);
- location information of the target (Cell Global Identity);
- time of event;
- Access Point Name (APN).

The below information is available when the intercept subject utilizes the GPRS service via the following events at the GPRS Support Nodes (e.g., SSGN, GGSN):

- GPRS attach;
- GPRS detach;
- PDP context activation;
- start of interception with PDP context active;
- PDP context deactivation;
- Call and/or Routing Area update;
- SMS

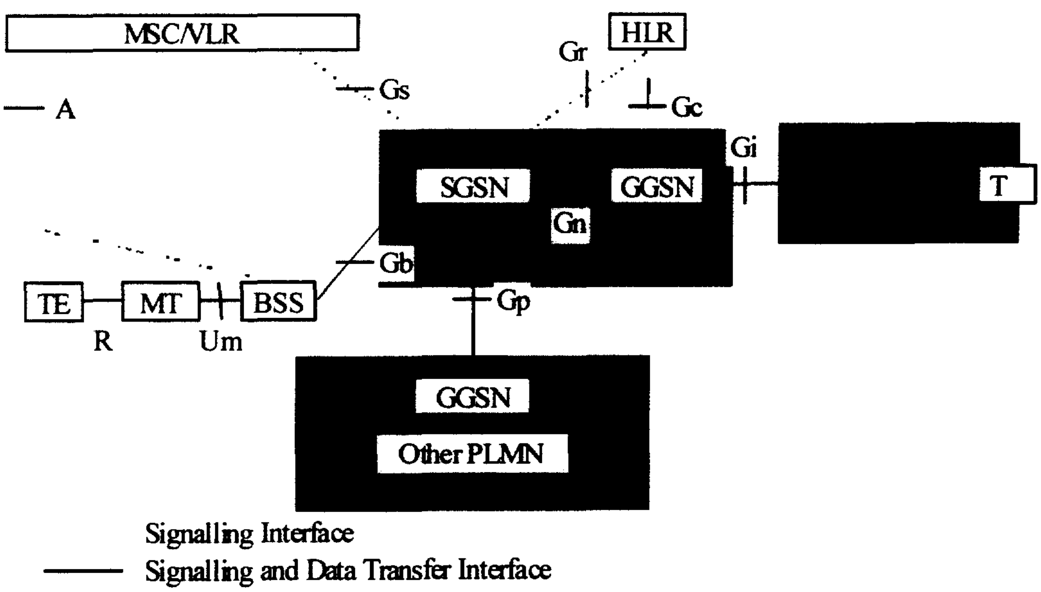

Figure 1. *GPRS Simplified GPRS Architecture*

The following areas where Call Identifying Information for Packet-mode Communication could be reported to assist Law Enforcement Agencies (LEAs) have been identified.

A.1.3.2 Reporting of Access Control Information

Similar to wireline, wireless systems establish a communication path across the accessing system from the subject's device to a network before communication between subject and associate can begin. The establishment and release of this path could be reported to identify when an intercept subject has established communication ability.

Specific to the issue of reporting information for Access Control as discussed above, the following specific information from the entire list of information available could be reported to law enforcement separately from the content to report the access event:

- access path ID (e.g., a PDP Context path);
- network access address (e.g., Access point Name);
- intercept subject address (e.g., IP address);
- either path establishment or path release (e.g., PDP Context Activation/Deactivation).

A.1.3.3 Reporting Packet Data Communication Addresses

After a communication path is established by a wireless accessing system between the subject device(s) and network, the subject can communicate directly with an associate over the connecting path. In this scenario the packet-mode communication, voice, or data, bypasses the call server of the accessing system and there would be no J-STD-025 type call events reported to the LEAs[4]. To assist LEAs in identifying the parties to the communication, the network addresses available to the accessing system could be reported. For example, with an IP network layer the source and destination addresses for the IP packet in the IP Header could be reported.

Specific to the issue of reporting information for identifying the parties to the communication as discussed above, the following specific information from the entire list of information available could be reported to law enforcement separately from the content to identify the addresses of the parties to the communication:

- access path ID (e.g., PDP Context path[5]);
- source address (e.g., IP Source Address[6]);
- destination address (e.g., OP Destination Address).

Access path ID is used to correlate path, source, and destination addresses.

---

[4] When packet mode voice calls involve the accessing system's call server, the call signaling events are reported and the reporting of packet header information would be redundant and unnecessary.

[5] Correlates Network Address Information to Access Path Events (e.g., PDP Context Activation/Deactivation).

[6] Either the source or destination address is associated with the intercept subject and thus indicates direction of packet flow.

A.1.4 Cellular Digital Packet Data

A.1.4.1 CDPD Architecture Overview

The CDPD Network operates as a collection of CDPD Service Provider Networks. The network architecture model shown in the diagram identifies the abstract functional elements.

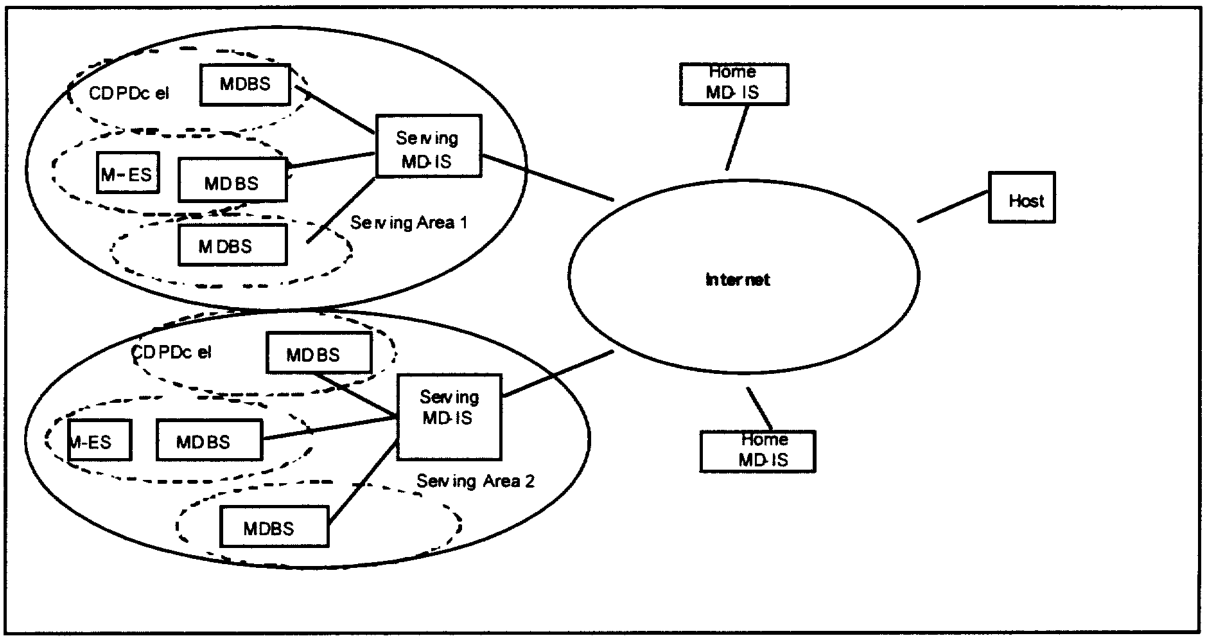

Figure 2. CDPD Network Architecture Model - functional elements

The CDPD specific Mobile Data Intermediate System (MD-IS) performs routing functions based on knowledge of the current location of the Mobile End-System (M-ES). The geographic grouping of cells connected to an MD-IS defines a serving area. Each serving area may cover multiple cellular radio coverage regions. Multiple serving areas may exist in a single CDPD service provider network. Multiple CDPD service provider networks are interconnected to provide seamless mobility routing for the mobile subscriber.

Mobility Management functions to support routing are localized in the following network entities:

- Mobile End System
  The Mobile End System (M-ES) is the means by which CDPD Network subscribers gain access to wireless communications. Each M-ES is aware of its location based on

broadcast information. When an M-ES powers up in a CDPD cell, it informs the network of its location using the registration process. When the M-ES moves to another cell, it notifies the network by indicating a change to new cell. When the M-ES moves to another cell in a new serving area, it performs a new registration.

- Mobile Data Base Station
  The MDBS provides Layer 2 data link or media access relay functions for a set of radio channels serving a cell. The MDBS does not participate in the wide area mobility management task.

- Home MD-IS
  Every M-ES address is logically a member of a fixed home area. The home area provides the anchor or mobility-independent routing destination area for routers and hosts that are not mobile aware (*i.e.*, routers and hosts on the general internet). The home MD-IS is responsible for transparently redirecting and forwarding data packets. The redirection and forwarding function is based on the principle of encapsulating M-ES addressed packets and forwarding them to the Serving MD-IS in each serving area the M-ES visits. In other words, data packets destined for the M-ES are routed through the general internet to the Home MD-IS. The Home MD-IS then encapsulates the packet and forwards the encapsulated packet to the appropriate Serving MD-IS. The Home MD-IS does not need to be involved in the routing of packets originated at the M-ES.

- Serving MD-IS
  The Serving MD-IS handles the routing of packets for all M-ESs in its serving area. When an M-ES registers for network access in an MD-IS serving area, the Serving MD-IS provides the Home MD-IS the current location of the M-ES. The serving MD-IS provides readdressing service by decapsulating forwarded data packets from the Home MD-IS and routes them to the correct radio cell. Data packets received from an M-ES and destined for a peer host are routed as in any internetwork, without the requirement of traversing the home MD-IS.

It should be noted that in the CDPD mobility management architecture, each network entity maintains a component of the complete information. The Home MD-IS maintains information regarding the M-ES to the detail of the serving area. Furthermore, the Home MD-IS does not have visibility to the data packets originated by the M-ES.

The Serving MD-IS maintains information regarding the location of M-ES to the resolution of a radio cell. The Serving MD-IS also routes all data packets destined to and originated from the M-ES. However, when the M-ES relocates to another serving area, the old Serving MD-IS is not informed of the new serving area.

A.1.4.2 Network Service

The CDPD network provides wireless mobile routing of network layer data packets. The CDPD System Specifications specifies support for two connectionless network layer protocols – Internet Protocol (IP) and Connectionless Network Protocol (CLNP). However, the currently deployed systems all support only IPv4.

The CDPD network has been defined to support the network protocol without any modification, as such the identity managed by mobility management is the IPv4 address. In other words, the subscriber identity is the IPv4 address, and is used for all routing purposes. There is no mapping of the target identity to the CDPD technology address.

Furthermore, since the CDPD network provides routing of connectionless network layer protocol data packets, there is no Call Management Service.

A.1.4.3 Information Provided

On the CDPD system, a Mobile End System (M-ES) must register with the network prior to establishment of data communications with peer entities. Therefore, at time of registration, the CDPD network shall provide the following information:

- Case identity
- Service Provider Network Identity of the serving system.
- Date and time of registration of the intercept subject.
- IP address of the intercept subject.

The CDPD mobility management procedure requires the M-ES to register when moving from one serving area to another. Therefore, if the intercept is provided at the Home MD-IS, the above information is provided whenever an M-ES moves to a new serving area. If the intercept is provided at the Serving MD-IS, the above information shall only be provided on entry of the M-ES into its serving area.

At the time of deregistration of the intercept subject, the CDPD network shall provide the following information:

- Case identity
- Service provider identifier of the serving system.
- Date and time of deregistration of the intercept subject.
- IP address of the intercept subject.

Once a CDPD M-ES has been registered, an intercept point at a Serving MD-IS shall provide the following on each IP packet delivered to, or received from the intercept subject:

- Case identity
- Date and time of receipt of the IP packet by the network
- Source and destination IP addresses of the intercepted packet
- The Cell Identifier of the location of the intercept subject M-ES (if available).

Once a CDPD M-ES has been registered, an intercept point at a Home MD-IS shall provide the following on each IP packet delivered to the intercept subject:

- Case identity

- Date and time of receipt of the IP packet by the network
- Source and destination IP addresses of the intercepted packet
- The Service Provider Network Identity of the serving system.

A.1.4.4 Feasibility and Performance

The TIA Interim Standard 732 (IS-732) has no provisions for the capabilities described in this report. Implementation feasibility of these capabilities will depend on each product's design. However, the industry believes that current CDPD products can be modified to supply the information described in this Appendix. These modifications would have limited impact on performance when the percentage of packets being intercepted is low.

A.1.5 Packet Cable

A.1.5.1 Introduction

PacketCable™, a project conducted by Cable Television Laboratories, Inc. (CableLabs®) and its member companies, is identifying and defining specifications which may be used to implement packet-based telephony, video, and other high speed, multimedia services over hybrid fiber coax (HFC) cable systems utilizing the DOCSIS protocol for access and the Internet Protocol (IP) for end-to-end data transport. This section is derived from Packet Cable Labs published standard for implementation of CALEA [PKT-PCES]. The JEM takes no position on any legal conclusions in this standard.. PacketCable utilizes a network superstructure that overlays the two-way data-ready broadband cable access network. While it is anticipated that the initial PacketCable service offering will be packet-based residential telephony, the long-term project vision encompasses a large family of packet-based services.

In recent years the growth of a worldwide IP based data network, coupled with the exponential growth in the number of households that have online access, have resulted in an enabling environment for offering integrated voice and data services over a common broadband cable access network and IP transport backbone. While the initial application of IP voice technology was for toll bypass services, the technology has now matured to the point where it is feasible to offer IP based voice services, including services that may substitute for local exchange services offered by traditional local exchange carriers, and even intelligent feature phone service for both voice and video.

With the success of the DOCSIS standardization effort, the QoS enhancements of DOCSIS 1.1, and the acceleration of major cable system upgrades for two way capacity, the infrastructure is in place for development and deployment of packetized voice and video applications. These applications can be deployed at relatively low incremental costs, providing a reasonable alternative to traditional local telephony, as well as a platform for introducing the next generation of telephony and general real time multimedia services.

Note that from time to time this section refers to the voice communications capabilities of a PacketCable network in terms of "telephony" or "IP Telephony." The legal/regulatory classification of IP-based voice communications provided over cable networks and otherwise, and the legal/regulatory obligations, if any, borne by providers of such voice communications, are not yet fully defined. Nothing in this section is addressed to, or intended to affect, those legal/regulatory issues. In particular, while this section uses standard terms such as "call," "call signaling," "telephony," "telephone number," etc., it should be recalled that while a PacketCable network performs activities analogous to these PSTN functions, the manner by which it does so differs considerably from the manner in which they are performed in the PSTN by telecommunications carriers, and that these differences may be significant for legal/regulatory purposes. Moreover, while reference is made here to "IP Telephony," it should be recognized that this term embraces a number of different technologies and network architecture, each with different potential associated legal/regulatory obligations. No particular legal/regulatory consequences are assumed or implied by the use of this or any other term derived from usage within the traditional circuit-switched telephone industry.

Note also that this section discusses the interface between a telecommunications carrier that provides telecommunications services to the public for hire using PacketCable™ capabilities (a "PacketCable/Telecommunications Service Provider," or "PC/TSP") and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. Companies using PacketCable capabilities will not in the normal case be "telecommunications carriers," either as defined in the Communications Assistance for Law Enforcement Act (CALEA) or otherwise. Instead, they will be providers of information services. However, some companies using PacketCable capabilities may, by virtue of other actions, be "telecommunications carriers" for purposes of CALEA with respect to their use of PacketCable capabilities. In this regard, a telecommunications carrier that complies with a publicly available technical requirement or standard adopted by an industry association or standards-setting organization shall be found to be in compliance with the assistance capability requirements of CALEA. As noted, cable operators are not ordinarily telecommunications carriers, but if a cable operator has taken the steps to become a carrier, and uses PacketCable to provide carrier services, then CALEA may apply to the equipment used to implement PacketCable. For this reason, we are providing consideration of CALEA concerns as part of the PacketCable specification, for the benefit of anyone who might use this architecture/technology as part of their carrier activities.

A.1.5.2 Architecture

The PacketCable reference architecture for PacketCable 1.0 is shown in Figure 1. The architecture can be divided into three phases. The access network on the originating client side, the managed IP Network with an interface to the PSTN and the access network on the terminating client side.

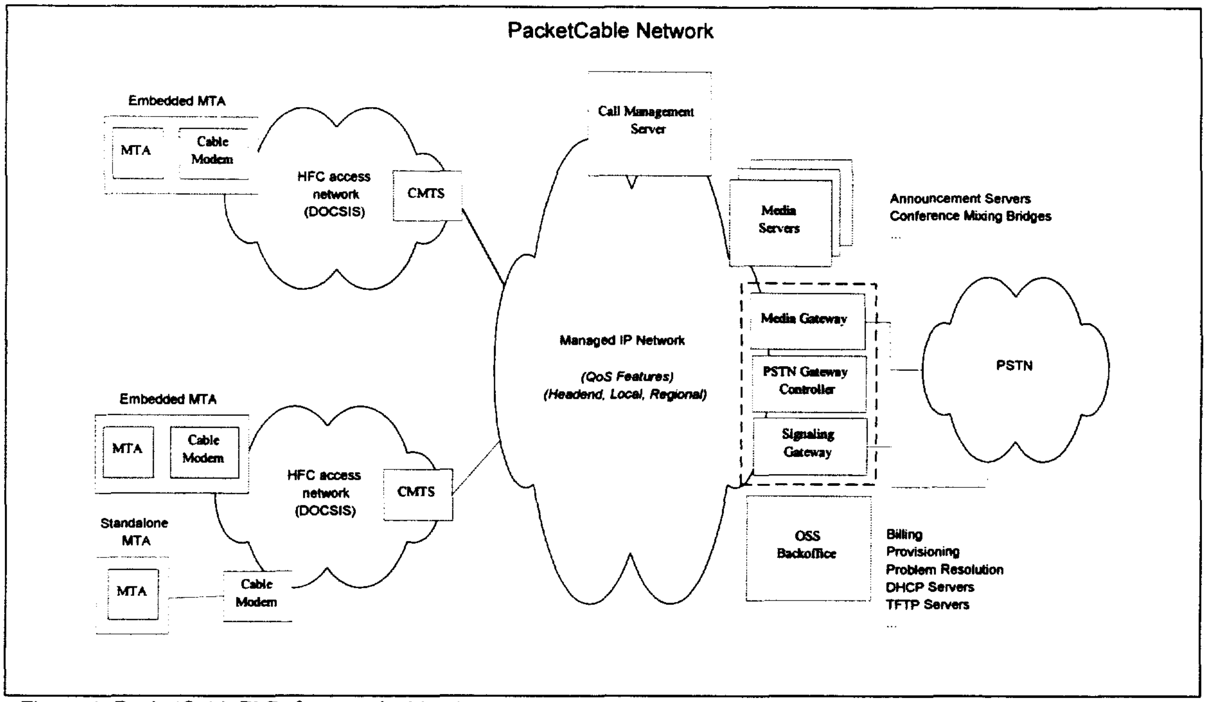

Figure 1. PacketCable™ Reference Architecture

The HFC DOCSIS access network as shown in Figure 2, provides the access to the managed IP network with DOCSIS 1.1 enabled Quality of service. The access network is defined to include the Cable Modem (CM), Multi-media Terminal Adapter (MTA), and the Cable Modem Termination System (CMTS). In PacketCable 1.0, the subscriber equipment consists of an embedded MTA with a DOCSIS CM MAC and PHY. The CMTS resides in the cable head end office and provides provisioning, authorization, and admission control for data communication over the access network.

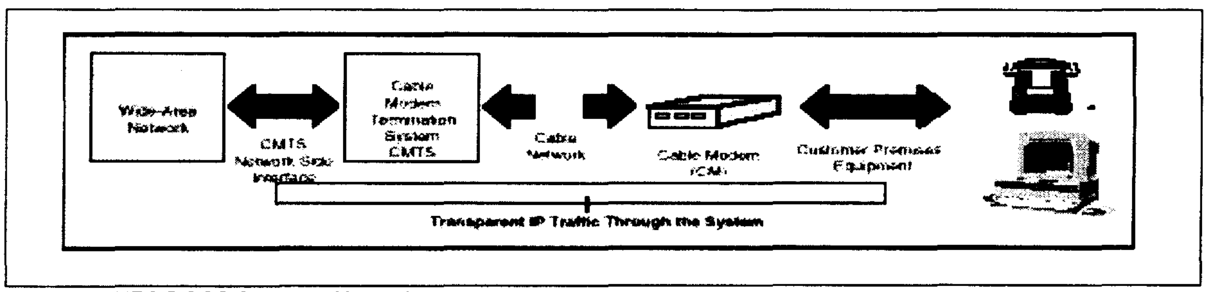

Figure 2: HFC DOCSIS Access Network

The PacketCable managed IP network provides interconnection between PacketCable network elements involved in call signaling, provisioning, and quality of service establishment, as well as long-haul IP connectivity to other PacketCable administrative domains. The managed IP network is defined to include the Call Management Server which contains a Call Agent to provide the telephony signaling services and a Gate controller which is a responsible for the admission policy decision. Announcement Server is used to manage and provide all announcements in the network.

The PSTN interface is a vital part of the PacketCable reference architecture. The PSTN interface consists of three main elements, the Signaling Gateway (SG) which translates signaling messages between the PSTN and IP network, the Media Gateway (MG) which translates media between the PSTN and IP network, and the Media Gateway Controller (MGC) which controls the access to the PSTN gateway.

A.1.5.3 Subscriber Equipment

The subscriber equipment includes those elements of the access network that are located in the customer's home. This includes the Cable Modem (CM) and the Multi-media Terminal Adapter (MTA).

The CM is a PacketCable network element as defined by the DOCSIS specification. The CM plays a key role in handling the media stream. Services, which may be provided by the CM, include classification of traffic into service flows according to classification filters, rate shaping, and prioritized queuing.

An MTA is a single hardware device that incorporates audio and optionally video IP telephony. An MTA may optionally incorporate a DOCSIS cable modem (an Embedded MTA) or may connect through external means to a DOCSIS cable modem (a Standalone MTA).

An MTA supports the following functionality:

- Provides one or more RJ11 interfaces to 2500-series phones
- Performs call signaling with the CMS to originate and terminate calls
- Supports QoS signaling with the CMS and the CMTS
- Supports security signaling with the CMS and other MTA devices
- Supports provisioning signaling with the Provisioning server(s)
- Performs encoding/decoding of audio streams
- Provides multiple audio indicators to phones, such as ringing tones, call waiting tones, stutter dial tone, dial tone, etc.
- Provides standard PSTN analog line signaling for audio tones, voice transport, caller-id signaling, and message waiting indicators.

The PacketCable system design places much of the session control intelligence at the endpoints, where it can easily scale with technology and provides new and innovative services. While this "future-proofing" is a goal of the design, we recognize that it leaves open a wide range of security threats. The basic assumption is that the MTA is not immune to customer tampering, and that the significant incentive for free service will lead to some very sophisticated attempts to thwart any network controls placed on the MTA.

Under these circumstances, it is important to realize that an MTA under customer control will likely not cooperate with electronic surveillance, and methods are therefore described here that do not depend in any way on cooperation with the MTA.

A.1.5.4 Subscriber Identification

A subscriber for electronic surveillance purposes is identified by a telephone number, and the telephone number is reported to Law Enforcement Agency (LEA) in the Pen Register and Trap and Trace information. Other identity information of the subscriber equipment, e.g. a provisioned security certificate, is used by the CMS to dynamically determine the identity of the subscriber and the telephone number for a particular call. The CMS includes, as part of the authorization of network resources, the packet stream identification (source and destination IP addresses, destination port number) and an indication that the packet stream is subject to surveillance.
Other mechanisms of subscriber identification are too dynamic and transient to be used as subscriber identification for surveillance.

Cable Modems (CMs) are manufactured with a unique MAC address (48-bits). This MAC address is used by DOCSIS to identify the CM during the registration process, and identifies a particular configuration file containing further provisioning information for the subscriber. The MAC address only appears on the HFC network, and is often suppressed by the Payload Header Suppression feature of DOCSIS. It is therefore not usable as a subscriber identifier for a 'snooping' function attached to the HFC network. Packet streams generated by the CM are identified by DOCSIS Service Flows. Each Service Flow has a dynamic identifier assigned, the Service-Flow-ID (SFID); while active it also has a Service-ID assigned (SID). The SID is used in the DOCSIS media access layer to control access to the shared upstream resources. The dynamic and transient nature of SIDs makes them unusable as subscriber identifiers for surveillance.

The CM uses DHCP to obtain an IP address. This resulting address is likely to change every time the CM is initialized. Use of a 'snooping' function on the IP links of the network would require dynamic configuration based on DHCP requests. This may be technically feasible, but has not been attempted in the PacketCable environment.

A.1.5.5 Intercept Access Points

The Intercept Access Function, performed by the Intercept Access Points (IAPs), isolates an intercept subject's communication or reasonably available Pen Register and Trap and Trace information unobtrusively. The Access Function is responsible for the collection of call content and reasonably available Pen Register and Trap and Trace information and making such information available to the Delivery Function.

In a PacketCable network, the following elements are possible Intercept Access Points:

- The Cable Modem Termination System (CMTS) which controls the set of cable modems attached to the shared medium of the DOCSIS network. The CMTS is responsible for intercepting the Call Content, and certain Pen Register and Trap and Trace information.
- The Call Management Server (CMS) which provides service to the subscriber. The CMS is responsible for intercepting the Pen Register and Trap and Trace information.

- The Media Gateway (MG) is designated as an Intercept Access Point for purposes of intercepting Call Content for redirected calls to the PSTN.
- The Media Gateway Controller (MGC) is designated as an Intercept Access Point for purposes of intercepting the Pen Register and Trap and Trace information for redirected calls to the PSTN.

The equipment and facilities of each subscriber include two Intercept Access Points (CMTS and CMS), and Pen Register and Trap and Trace information reasonably available at these IAPs is provided to LEA. Redirected calls in the PacketCable network might not utilize the equipment or facilities of the subscriber who initiated the redirection. Accordingly, the Intercept Access point for a call that has been redirected will be either the CMS/CMTS of the new destination (if redirected to another PacketCable endpoint within the same provider's network) or the MGC/Media Gateway of the PSTN interconnection (if redirected to a PSTN endpoint).

A.1.5.6 Information Available to Law Enforcement

For purposes of the PacketCable network's surveillance capabilities, only those packets sent or received by the intercept subject that utilize the capabilities of the Call Management Server to establish the communication, and utilize enhanced Quality of Service as authorized by the Call Management Server, are considered "calls" within the scope of surveillance support obligations set out in CALEA. Cable operators that have deployed PacketCable capabilities may offer a range of other services to their customers that make use of packet-switched communications, such as email and Internet access. Other than the packets identified in the first sentence of this paragraph, packets sent or received by the intercept subject are considered Information Services.

The following call events are defined, and convey information to an LEA for Pen Register and Trap and Trace events: Answer (a two-way connection has been established for a call under surveillance), Change (a change in the description of call content delivery for a call under interception), Close (end of call content delivery for a call under interception), Open (beginning of call content delivery for a call under interception), Origination (IAP detects that the surveillance subject is attempting to originate a call), Redirection (call under surveillance is redirected, e.g. via termination special service processing, or via a call transfer), and Termination Attempt (IAP detects a call attempt to a surveillance subject).

In most cases, a PC/TSP should be able to intercept calls redirected by a surveillance subject to other locations either in its own network or in the networks of other telecommunications carriers. However, where a subject has redirected incoming calls to a location served by another PC/TSP, the resulting connection may be established without touching the equipment or facilities of the subject's PC/TSP. Instead, the connections will be made directly from the PC/TSP originating the incoming call to the PC/TSP serving the location to which the subject redirected incoming calls. Because the subject's original PC/TSP will not be aware of these resulting connections, access to these connections will have to be obtained from the PC/TSP serving the location to which calls have been redirected.

Communications in progress at the time a PC/TSP receives a legally authorized request will not be subject to surveillance. Only communications initiated after the legally authorized request will be subject to surveillance.

A.1.5.6.1. Reporting Access Control Information

For Packet Cable managed IP network the following information could be reported:

- subject identity;
- target identity;
- access element identity;
- time of event;
- call identity unique to this call;
  - originating Session Descriptor Protocol information;
  - terminating Session Descriptor Protocol information;
  - call content connection identifier for Title lll warrants;
  - redirected information;
  - origination digits
  - termination digits and
  - the transit carrier used to transport the session;

A.1.5.7 Preferred Delivery Format

The network layer protocol for delivery of both Call Data Connection (CDC) and Call Content Connection (CCC) information is as defined by the Internet Protocol (IP) [RFC0791]. Both CCC and CDC information may be provided over the same physical interface. Information is available in the CCC and CDC information packets to identify the type of packet (either CDC or CCC) and the particular case. The identification is provided either directly by the packet containing the surveillance case identifier, or indirectly by the packet containing an identifier that can be correlated with the case identifier.

Call Content is delivered as a stream of UDP/IP datagrams, as defined in [RFC0768, RFC0791], sent to the port number at the Collection Function (CF) as provided during provisioning of the interception. The format of the UDP/IP payload is given in the PacketCable Electronic Surveillance Specification.

The Call Data Connections in PacketCable are implemented as TCP/IP connections, established by the Delivery Function (DF), to the Collection Function designated by the LEA in the surveillance provisioning.

Contained in the IP header is the source IP address, which is the address of the DF, and the destination IP address, which is the address of the CF provided during interception provisioning.

All transfer of packets other than those operationally required to maintain the link are from the Delivery Function to the Collection Function only. At no time may the LEA send unsolicited packets from the CF to the DF.

The default link-layer protocol between the DF and CF is as defined by the Ethernet protocol [RFC0894, RFC0826]. However, alternate link-layer protocols may be used at the discretion of the PC/TSP based on negotiated agreements with the LEA.
The default type of physical interconnect provided by the PC/TSP at the demarcation point is an RJ45 10/100BaseT [ISO8802-3] connection. However, alternate physical interconnects may be provided at the discretion of the PC/TSP.

A.1.5.8 Capacity Limitations

Capacity requirements are fundamental to the design and development of any technical standard or specification (as well as for the equipment developed in compliance with such standards). Several technical considerations, pivotal to the design process, are affected by capacity requirements. However, so far, the Attorney General has not identified capacity requirements for telecommunications carriers that use PacketCable capabilities to provide telecommunications services. In the absence of these formal capacity requirements, CableLabs has had to make certain reasonable assumptions about capacity in order to proceed with developing this specification. CableLabs believes that these assumptions reflect reasonable estimates based on industry's technical expertise as well as law enforcement's historical requirements on other technologies. However, to the extent that these reasonable assumptions differ from whatever formal capacity requirements the Attorney General eventually identifies, substantial modifications to this specification may be required (with resulting delays and lost effort in the design and development of equipment consistent with this specification).

As such, PacketCable has made the following assumptions: (1) the IAP supports a maximum number of intercepts of 5% of its active calls, (2) the DF supports a maximum of five surveillance orders for any single subject, (3) the DF to CF interface must be capable of supporting the maximum number of intercepts times the maximum number of intercepts per subject, (4) it is the responsibility of the PC/TSP to provide adequate resources to transport call content and call data information from the IAP to the DF based on statistical call models, (5) it is the responsibility of the PC/TSP to provide adequate resources to transport redirected call content and call data information between DFs within the PC/TSP network based on statistical call redirection models, (6) when adequate resources are not available, situations may arise where call content and Pen Register and Trap and Trace information are not delivered to the LEA.